IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

AMANDA MARCONI, R.M., a minor, by and through her legal guardian Amanda Marconi, CORY COYLE, and PATRICK NEALON, Individually and on behalf of all others similarly situated, Plaintiffs, v. NORTHWELL HEALTH, INC., and PERRY JOHNSON & ASSOCIATES, INC., Defendants.	CLASS ACTION COMPLAINT Case No.: _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Amanda Marconi, R.M., a minor, by and through her parent and legal guardian Amanda Marconi, Cory Coyle, and Patrick Nealon (collectively "Plaintiffs") on behalf of themselves and all others similarly situated, by and through their undersigned attorneys, bring this Class Action Complaint against Defendants Northwell Health, Inc. ("Northwell") and Perry Johnson & Associates, Inc. ("PJA") (individually, and collectively, "Defendants"), and allege, upon personal information and belief and their counsels' investigations,[1] that Defendants failed to secure and safeguard current and former patients' personally identifiable information, including highly sensitive information such as their name, social security number, date of birth, address, medical record number, hospital account number, and clinical information, such as the

[1] Plaintiffs' Counsel is engaging in an active investigation into the data breach referenced in Defendants' Notice of Data Breach dated November 3, 2023 (the "Data Breach").

name of treatment facilities, the name of healthcare providers, admission information, diagnoses, and date(s) and time(s) of services (collectively, "PII").

Plaintiffs and Class Members entrusted Defendants with their highly sensitive PII and reasonably expected Defendants to securely collect and safeguard their PII. Defendant Northwell knowingly employed third-party vendor PJA to maintain its patients' highly sensitive PII. Defendants knew patients' PII, including confidential health information, which is highly sought after by hackers and cybercriminals, is extremely valuable information. For this reason, Defendants knew or should have known that reasonable measures must be employed to protect Plaintiffs' and Class Members' highly sensitive PII from unauthorized disclosure. Defendants failed to fulfill that responsibility to Plaintiffs and Class Members (defined below). Defendants also failed to provide timely, accurate, and adequate notice to Plaintiffs and Class Members that their sensitive health information and PII had been compromised in a data breach, as well as precisely what types of information were taken. As a result of Defendants' misconduct, Plaintiffs suffered damages.

INTRODUCTION

1. Defendant Northwell is New York State's largest healthcare provider, operating over 20 hospitals and 890 outpatient facilities and serving over two million patients in the New York metropolitan area.

2. Defendant PJA is a vendor Defendant Northwell hired to provide transcription and dictation services in furtherance of Defendant Northwell's medical practice. As part of PJA's relationship with Northwell, PJA received scores of Plaintiffs' and Class Members' PII, including confidential health information.

3. Defendants are responsible for securing, safeguarding, and maintaining Plaintiffs' and Class Members' highly sensitive PII, but Defendants failed to fulfill their duty.

4. Beginning on March 27, 2023, an unauthorized third party gained access to PJA's network, containing Plaintiffs' and Class Members' highly sensitive PII.

5. Defendant PJA failed to discover its network vulnerability and the unauthorized access to its systems by a third party until May 2, 2023.

6. Defendant Northwell learned of PJA's network vulnerability and the unauthorized access to PJA's systems by a third party on July 21, 2023.

7. Because Defendants failed to identify PJA's network vulnerability and the unauthorized access for months, Plaintiffs' and Class Members' PII was accessed, viewed, downloaded, or stolen.

8. Defendants failed to provide timely notice of the Data Breach to Plaintiffs and Class Members. Indeed, Plaintiffs and Class Members did not receive any notice of the Data Breach until on or about November 3, 2023. Defendants' extensive delay in notifying Plaintiffs and Class Members of the Data Breach violates the immediate notice requirement of N.Y. Gen. Bus. Law § 899-aa, and renders Defendants' purported privacy assurances material misrepresentations in violation of N.Y. Gen. Bus. Law §§349, 350.

9. Worse yet, the notice of the breach came from Defendant PJA and not directly from Defendant Northwell.

10. To date, Defendants' notice of the Data Breach has been wholly insufficient because it fails to disclose who the unauthorized third party is, the full scope of the data impacted by the Data Breach, the precise PII that was breached, and the time period from which the PII was originally collected by Defendant Northwell.

11. Defendants were acutely aware of the risk of cyber-attacks, data breaches, and unauthorized disclosures to their systems. Indeed, Defendant Northwell assured the public that

"Northwell Health understands" patients' "concerns about privacy" and claimed it was taking steps to protect their PII.

12. Based on Defendants' representations, Plaintiffs and Class Members entrusted their highly sensitive PII to Defendants at a time when the healthcare industry is a central target of cybercriminals due to their storage of vast amounts of PII, including confidential health information.

13. Defendant Northwell is aware of the signs and risks of data breaches and cyber-attacks, having faced other similar breaches in the past.

14. Despite Defendants' awareness of the foreseeable risk of data breaches, cyber-attacks, and unauthorized access by third parties, Defendants failed to implement reasonable security or privacy systems or measures to protect Plaintiffs' and Class Members' highly sensitive PII from unauthorized access or disclosure.

15. Because of Defendants' unreasonable security protocols and untimely notice of the Data Breach, Plaintiffs and Class Members face an increased (and imminent) risk of identity theft and fraud. In fact, Plaintiffs and Class Members may have already suffered from identity theft and fraud.

16. Now, Plaintiffs and Class Members are forced to take affirmative steps to protect themselves against the imminent risk of identity theft or fraud that they would not otherwise have had to take, such as (i) implementing credit freezes; (ii) setting alerts with credit reporting agencies; (iii) alerting financial institutions; (iv) alerting medical providers; (v) closing or modifying bank accounts; or (vi) monitoring credit reports for unauthorized activity.

17. Plaintiffs and Class Members have been and will continue to be injured by Defendants' failure to safeguard their highly sensitive PII. In addition to having their privacy

invaded, Plaintiffs and Class Members face an imminent risk of identity theft or fraud. Moreover, because Defendants have failed to ascertain the full scope of the Data Breach, Plaintiffs are unable to sufficiently mitigate the imminent risks of identity theft or fraud that they currently face.

18. To date, Defendants maintain possession, custody, and control over Plaintiffs' and Class Members' highly sensitive PII, but Plaintiffs and Class Members have no way to safeguard their highly sensitive PII from further disclosure. Thus, Plaintiffs and Class Members face a continued, unknown risk of additional harm which will only be revealed upon Defendants' completion of their investigation.

PARTIES

19. Plaintiff Amanda Marconi ("Plaintiff Marconi") is a resident and citizen of the State of New York and a patient of Northwell. Plaintiff has been a patient of Northwell for approximately the past four years. Plaintiff provided her highly sensitive PII to Defendants in order to receive healthcare services. Plaintiff provided her highly sensitive PII, which included medical information, based on the reasonable assumption that Defendants would secure and safeguard her PII with adequate security and privacy measures and protect her PII from unauthorized disclosure. Further, Plaintiff provided her PII based on the reasonable assumption that Defendants would promptly and timely notify her of any unauthorized disclosure of her PII to mitigate, among other things, the risks of identity theft and fraud. As a result of Defendants' misconduct, which caused the Data Breach, Plaintiff is taking and will continue to take measures that she would not otherwise have to take to ensure that her identity is not stolen, accounts are not compromised, and personal data is not used for illegal purposes. Additionally, as a result of Defendants' misconduct, which directly and proximately caused the Data Breach, Plaintiff did not get what she bargained for.

20. Plaintiff R.M. ("Plaintiff R.M.") is a resident and citizen of the State of New York and a patient of Northwell. Plaintiff has been a patient of Northwell for approximately the past four years. Plaintiff provided her highly sensitive PII to Defendants in order to receive healthcare services. Plaintiff provided her highly sensitive PII, which included medical information, based on the reasonable assumption that Defendants would secure and safeguard her PII with adequate security and privacy measures and protect her PII from unauthorized disclosure. Further, Plaintiff provided her PII based on the reasonable assumption that Defendants would promptly and timely notify her of any unauthorized disclosure of her PII to mitigate, among other things, the risks of identity theft and fraud. As a result of Defendants' misconduct, which caused the Data Breach, Plaintiff is taking and will continue to take measures that she would not otherwise have to take to ensure that her identity is not stolen, accounts are not compromised, and personal data is not used for illegal purposes. Additionally, as a result of Defendants' misconduct, which directly and proximately caused the Data Breach, Plaintiff did not get what she bargained for.

21. Plaintiff Cory Coyle ("Plaintiff Coyle") is a resident and citizen of the State of New York and a patient of Northwell. Plaintiff has been a patient of Northwell since approximately 2015. Plaintiff provided his highly sensitive PII to Defendants in order to receive healthcare services. Plaintiff provided his highly sensitive PII, which included medical information, based on the reasonable assumption that Defendants would secure and safeguard his PII with adequate security and privacy measures and protect his PII from unauthorized disclosure. Further, Plaintiff provided his PII based on the reasonable assumption that Defendants would promptly and timely notify him of any unauthorized disclosure of his PII to mitigate, among other things, the risks of identity theft and fraud. As a result of Defendants'

misconduct, which caused the Data Breach, Plaintiff is taking and will continue to take measures that he would not otherwise have to take to ensure that his identity is not stolen, accounts are not compromised, and personal data is not used for illegal purposes. Additionally, as a result of Defendants' misconduct, which directly and proximately caused the Data Breach, Plaintiff did not get what he bargained for.

22. Plaintiff Patrick Nealon ("Plaintiff Nealon") is a resident and citizen of the State of New York and a patient of Northwell. Plaintiff has been a patient of Northwell since at least as early as 2014. Plaintiff provided his highly sensitive PII to Defendants in order to receive healthcare services. Plaintiff provided his highly sensitive PII, which included medical information, based on the reasonable assumption that Defendants would secure and safeguard his PII with adequate security and privacy measures and protect his PII from unauthorized disclosure. Further, Plaintiff provided his PII based on the reasonable assumption that Defendants would promptly and timely notify him of any unauthorized disclosure of his PII to mitigate, among other things, the risks of identity theft and fraud. As a result of Defendants' misconduct, which caused the Data Breach, Plaintiff is taking and will continue to take measures that he would not otherwise have to take to ensure that his identity is not stolen, accounts are not compromised, and personal data is not used for illegal purposes. Additionally, as a result of Defendants' misconduct, which directly and proximately caused the Data Breach, Plaintiff did not get what he bargained for.

23. Northwell is a New York not-for-profit corporation headquartered at 2000 Marcus Avenue, New Hyde Park, NY 11042.

24. PJA is Nevada company headquartered at 1489 W Warm Springs Rd, Henderson, NV 89014. PJA offers transcription services to clients in the medical and legal industries as well as government agencies.

JURISDICTION & VENUE

25. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

26. The Eastern District of New York has personal jurisdiction over Defendants named in this action because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in New York and this District through their headquarters, offices, parents, and affiliates. Specifically, Defendant Northwell maintains its headquarters in New Hyde Park, New York. Defendant PJA, a third-party vendor of Northwell, serving Northwell's patients, conducted substantial business in New York by collecting and maintaining data of an estimated 3.8 million Northwell patients, including those located in this District.

27. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants and/or their parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

I. NORTHWELL ROUTINELY COLLECTS HIGHLY SENSITIVE PII FROM MILLIONS OF PATIENTS

28. Northwell is New York State's largest healthcare provider, operating over 20 hospitals and 890 outpatient facilities and serving over two million patients in the New York metro area.

29. Northwell, a highly sophisticated healthcare provider, touts its reputation as "NY's top choice for care" stating "[m]ore people choose Northwell than any other health system in the state [ ] – because New Yorkers know that where they go for care matters."[2]

30. In order to provide health services, Defendant Northwell collects, stores, and maintains scores of data from its patients. Northwell's Privacy Policy states:[3]

> How we collect your information
>
> We collect the information you provide directly to us. For example, we collect information when you:
>
> - Create an account
> - Access or use the Services
> - Pay your patient account statements
> - Schedule an appointment in the outpatient department of a Northwell hospital
> - Contact us with inquiries and comments
> - Complete and submit forms offered on the Services

31. As part of the above-listed processes, Northwell collects a wide variety of highly sensitive PII, including:[4]

- Name;
- Social Security Number;

[2] Northwell Health, https://www.northwell.edu/ (last visited Nov. 20, 2023).
[3] Northwell Health, *Privacy Policies & Disclaimers* (2023), https://www.northwell.edu/privacy-policies-disclaimers (last visited Nov. 20, 2023).
[4] *Id.*

- Address;
- Birthday;
- Age;
- Medical symptoms;
- Medical conditions;
- Medical test results;
- Diagnoses;
- Prescription information;
- Treatment facilities;
- Referrals;
- Medical records;
- Physician information;
- Insurance information; and
- Payment information.

32. This information is highly sensitive and includes confidential medical information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) – a federal law aimed at protecting sensitive patient health information from being disclosed without the patient's consent or knowledge.

33. Because of HIPPA and other laws requiring the protection of PII, Defendants had a duty to adopt reasonable measures to protect the PII, which included confidential health information, of Plaintiffs and Class Members from unauthorized access or disclosure to third parties.[5]

[5] Defendant PJA assumed a duty to Plaintiffs as a vendor and agent of Defendant Northwell.

34. Defendants were also obligated to take steps to fulfill the representations they made to the public about their ability to secure and safeguard PII, as discussed herein.

II. NORTHWELL TOUTED THE SAFEGUARDS IT PUT IN PLACE TO PROTECT PATIENT PII

35. Defendants understand their duty to protect patient health information from unauthorized disclosure and admit "that patient privacy is an integral part of the health care" it provides to its patients.[6]

36. Defendants' duty to safeguard Plaintiffs' and Class Members' PII arises from HIPPA, other state and federal laws, common law, industry standards, and Defendants' own public representations concerning cybersecurity and privacy.

37. Indeed, Defendant Northwell assured the public that "Northwell Health understands" patients' "concerns about privacy."[7] Northwell further assured patients that it was taking steps to protect their PII. Specifically, Northwell repeatedly represented that:

> we have many safeguards to protect the privacy and security of your personal information. For example, each of our facilities has a Privacy Officer who is able to answer any questions a patient may have about the way in which their health information will be used. ***We also have many policies in place to protect the privacy and security of your personal information and our employees are educated from the moment they are hired and continually after, to respect and protect our patient's privacy***. [8]

38. Additionally, Northwell provided patients with specific detail regarding the level of safeguards it employed to protect patients' highly sensitive PII from unauthorized disclosure. Northwell's Privacy Policy states:

> ***We employ commercially reasonable measures to safeguard the collection, transmission and storage of the information we collect***. These measures vary based on the sensitivity of the information that we collect,

---

[6] Northwell Health, *Protecting Patient Privacy*, https://www.northwell.edu/about-northwell/commitment-to-excellence/protecting-patient-privacy (last visited Nov. 20, 2023).
[7] *Id.*
[8] *Id.* (emphasis added)

> process and store and the current state of technology. ***We use software programs to monitor traffic to identify unauthorized attempts to upload or change information or other types of malicious use***. Information collected from these sources may be used to help identify an individual in the event of a criminal investigation or as required by any legal process. [9]

39. Defendant Northwell continues to tout its security and privacy measures to the public ***even after the Data Breach occurred***. As of about November 8, 2023, Northwell was still sending patients, Plaintiffs, and Class Members materials titled "We'd like to help you protect your identity."[10] The materials include a link to Defendant Northwell's website to "[l]earn how Northwell Health works to protect your identity."[11]

40. For the reasons stated herein, Plaintiffs and Class Members entrusted the sophisticated Defendants with their highly sensitive PII to receive healthcare services. Plaintiffs and Class Members relied on Defendants' reassuring disclosures that their highly sensitive PII would be protected from unauthorized disclosure when Plaintiffs and Class Members entrusted Defendants with their highly sensitive PII.

III. DEFENDANT PJA, AN AGENT OF NORTHWELL, HAD A DUTY TO SAFEGUARD PII

41. Defendant PJA confirms that it is a vendor of Defendant Northwell and its subsidiaries and affiliates.

42. Defendant Northwell hired Defendant PJA as a vendor to facilitate medical treatment. Specifically, Defendant Northwell hired Defendant PJA to provide transcription and dictation services in furtherance of Defendant Northwell's medical practice.

43. In order to provide Defendant Northwell with transcription and dictation services, Defendant PJA received transmissions of highly sensitive PII, which included Plaintiffs' and

---

[9] Northwell Health, *supra* note 3 (emphasis added).
[10] Marketing Materials from Northwell, attached hereto as Exhibit B.
[11] *Id.*

Class Members' confidential health information. Defendant PJA was responsible for securely maintaining and safeguarding the highly sensitive PII that it received from Defendant Northwell.

44. Thus, Defendant PJA had a duty to safeguard and maintain the confidentiality of Plaintiffs' and Class Members' highly sensitive PII, which included confidential health information.

45. Moreover, Defendant Northwell had a duty to employ vendors with reasonable security and privacy measures in place sufficient to safeguard Plaintiffs' and Class Members' PII.

IV. DEFENDANTS FAILED TO REASONABLY SAFEGUARD PATIENT PII AGAINST A DATA BREACH

46. On or about November 3, 2023, Defendants sent Plaintiffs and Class Members a *Notice of Data Breach*.[12] Defendants informed Plaintiffs and Class Members of the following information:

> **Who Is PJ&A and Why Did We Have Your Information?** PJ&A serves as a vendor to Northwell Health, Inc., and its subsidiaries and affiliates (collectively, "Northwell"). PJ&A provides certain transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding Northwell patients.
>
> **What Happened.** PJ&A became aware of a data security incident impacting our systems on May 2, 2023. We immediately initiated an investigation and engaged a cybersecurity vendor to further provide support in connection with our investigation and secure against potential system vulnerabilities. We promptly implemented the cybersecurity vendor-recommended actions to prevent the further disclosure of data as we continued to investigate the situation. Through our investigation, we determined that the unauthorized access to our systems occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.
>
> On July 21, 2023, PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A had

[12] Letter from PJ&A (Nov. 3, 2023), attached hereto as Exhibit A.

> preliminarily determined that Northwell data was impacted on May 22, 2023 and, by September 28, 2023, confirmed the scope of the Northwell data impacted.
>
> **What Information Was Involved.** We have confirmed that certain files containing your personal health information were impacted by this incident. Specifically, the following information may have been impacted: your name, date of birth, address, medical record number, hospital account number, and clinical information, such as the name of the treatment facility, the name of your healthcare providers, admission diagnosis, and date(s) and time(s) of service.

47. Defendants provided this notice to Plaintiffs and Class Members ***more than seven months after*** the start of the Data Breach. By Defendants' own admission, the breach began on or about March 27, 2023, during which time an unauthorized party gained access to, viewed, and downloaded Plaintiffs' and Class Members' PII on PJA's network.

48. Defendant Northwell was notified of the Data Breach on July 21, 2023 – three months after the breach and more than one hundred days before Plaintiffs and Class Members received the *Notice of Data Breach*. Defendants' extensive delay in notifying Plaintiffs and Class Members of the Data Breach violates the immediate notice requirement of N.Y. Gen. Bus. Law § 899-aa, and renders Defendants' security and privacy assurances material misrepresentations in violation of N.Y. Gen. Bus. Law §§349, 350.

49. Defendants have not offered any explanation for the extensive delay in providing Plaintiffs and Class Members with the *Notice of Data Breach*.

50. In initial announcements, Defendants reported that PII of more than 3.8 million individuals was compromised. Since that report, Defendant PJA disclosed that over 8 million

individuals were impacted by the Data Breach.[13] Defendants' investigation into the Data Breach is ongoing and is likely to reveal the existence of additional impacted individuals and data.[14]

51. The size and scope of this Data Breach is undoubtedly vast. Indeed, media outlets are referring to this Data Breach as "one of the largest healthcare data breaches ever discovered."[15]

52. The scope of the Data Breach will only be made worse by Defendants' ongoing investigation and the likely discovery of additional affected individuals.

53. Because Defendants' investigation is still ongoing, Plaintiffs and Class Members have no way of knowing the full impact of the Data Breach and the extent to which their highly sensitive PII has been misused.

54. On information and belief, the highly sensitive PII Defendants failed to safeguard was unencrypted, which has made or will make it easier for cybercriminals and hackers to misuse Plaintiffs' and Class Members' PII. Such PII has already been accessed and viewed by unauthorized third parties.

55. Since notifying patients about the Data Breach, Defendants claims that they "are committed to maintaining the privacy and security of [patients'] information and take the incident very seriously."[16] However, Defendants have failed to provide sufficient details about the cause of the Data Breach, the vulnerabilities hackers and/or cybercriminals exploited, the unauthorized third party or parties that initiated the cyber-attack, and the remedial measures undertaken to ensure a breach does not occur again.

---

[13] HIPAA Journal, *N.Y.'s Largest Health System Affected by PJ&A Data Breach* (Nov. 13, 2023), https://www.hipaajournal.com/northwell-health-pja-data-breach/..
[14] *Id.*
[15] *Id.*
[16] Exhibit B, *supra* note 10.

56. This information and the full scope of the Data Breach – which is not yet known – is critical to Plaintiffs and Class Members, in part, because Defendants continue to maintain possession, custody, and control over Plaintiffs' and Class Members' PII.

57. The *Notice of Data Breach* Plaintiffs and Class Members received is inadequate. Defendants fail to provide specific details about the breach that are necessary for Plaintiffs and Class Members to mitigate the imminent risk of identity theft and fraud. Specifically, Defendants have failed to: (i) disclose or identify the unauthorized third party; (ii) disclose the network or system vulnerabilities that allowed the unauthorized third party to gain access to Plaintiffs' and Class Members' PII, including confidential health information; (iii) disclose whether Defendants paid a ransom cost to recover any compromised PII; and (iv) specify the scope of the Data Breach, including the time period during which the compromised data was accessed or collected.

58. Plaintiffs' and Class Members' PII has been compromised and is likely to be misused by: (i) being put up for sale on the dark web; (ii) being exploited by criminals for illegal purposes; or (iii) being used for targeted marketing without Plaintiffs' and Class Members' knowledge or consent.

59. Upon information and belief, Defendants did not use reasonable security procedures and practices commensurate with the highly sensitive nature of the PII Plaintiffs and Class Members trusted Defendants to safeguard.

V. PATIENTS' COMPROMISED DATA IS HIGHLY VALUABLE TO HACKERS AND CYBERCRIMINALS

60. Cyberattacks by hackers and cybercriminals are pervasive and rapidly increasing in frequency. In a recent report, Forbes stated that the number of data breaches exceeded 422 million in 2022 and that the dark web has grown over 300% since 2017.[17]

61. The healthcare industry is acutely aware that their systems are a central target of cybercriminals due to their storage of vast amounts of PII, including confidential health information. Healthcare data breaches are occurring with increased frequency because healthcare systems have increased their use of digital services to store patient PII.[18] Recent reports confirm that:

> [i]n healthcare, cyberattacks have outpaced other industries as criminals seize the opportunity to exploit system vulnerabilities in pursuit of a trove of private medical information. Over the past five years, hacking incidents have skyrocketed, according to federal records [from the U.S. Department of Health and Human Services]. The records also say that, from 2010 to 2022, data breaches exposed 385 million patient records.[19]

62. Patient PII is highly valuable to hackers. Recent studies show that hackers value PII over other categories of data, such as credit card information and passwords. Accordingly, "PII is the most valuable since criminals can compile more PII from the dark web to then engage in harder to prevent fraud or full-on identity theft."[20]

---

[17] Forbes, *Why Data Breaches Are Increasing And What CISOs Can Do About It* (Apr. 20, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/04/20/why-data-breaches-are-increasing-and-what-cisos-can-do-about-it/?sh=7e83992c547e.
[18] Healthcare Drive, *Tracking Healthcare Data Breaches* (Nov. 15, 2023), https://www.healthcaredive.com/news/tracking-healthcare-data-breaches-cybersecurity-hacking-hospitals/696184/.
[19] *Id.*
[20] SC Media, *Hackers Went After Personally Identifiable Information the Most, Study Says* (Jan. 5, 2023), https://www.scmagazine.com/news/hackers-went-after-personally-identifiable-information-the-most-study-says.

63. Hackers and cybercriminals seek to amass PII because individual data points can "be pieced together like a puzzle" to "complete an online profile of" a person and "impersonate you or others online."[21] In addition to seeking PII for identity theft, hackers seek PII to sell and profit off of PII on the dark web.

64. Experian describes the dark web as "a huge marketplace for stolen data and personal information. After a data breach or hacking incident, personal information is often bought and sold on the dark web."[22] For this reason, Plaintiffs and Class Members face an imminent risk of having their PII – which was accessed, viewed, and downloaded in connection with this Data Breach – sold on the dark web.

65. Consumer data is highly valuable on the dark web. According to CyberDefense Magazine, "[o]n average, a consumer's passwords sell for around $80, while even small details like purchase history can sell for $20. Credit card numbers can sell for as little $5, while passports might fetch up to $2,000."[23]

66. Similarly, health and medical information are also valuable on the dark web. Reports indicate that in 2015, nearly 100 million healthcare records were compromised, reflecting criminals' demand for this information.[24] According to a recent study by Experian, medical records are among the top ten most valuable PII records to cybercriminals, valued

---

[21] Cyber Defense Mag., *What is PII and Why Criminals Want Yours* (2023), https://www.cyberdefensemagazine.com/what-is-pii-and-why-criminals-want-yours/.
[22] Experian, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[23] Cyber Defense Magazine, *supra* note 21.
[24] CyberPolicy, *Why Medical Records are 10 Times More Valuable Than Credit Card Info*, https://www.cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info#:~:text=Health%2C%20Wealth%20%26%20Cybercrime,be%20used%20for%20tax%20fraud!

between $1 to $1,000.[25] The following graphic depicts other valuable categories of PII, many of which were implicated by this Data Breach:[26]

67. Again, medical information is among the most valuable types of PII to cybercriminals and "is worth between 10 and 40 times more than your credit card number on the black market." Specifically, medical information can be used by cybercriminals for tax fraud purposes and to illegally obtain drugs.[27]

[25] Experian, *supra* note 22.
[26] *Id.*
[27] CyberPolicy, *supra* note 24.

68. Defendant Northwell is well aware of the cyber risks that healthcare organizations face. The risks are especially well-known because Defendant Northwell has previously experienced other data breaches and cyber-attacks.[28]

VI. DEFENDANTS FAILED TO EMPLOY REASONABLE SAFEGUARDS FOR PLAINTIFFS' AND CLASS MEMBERS' PII

69. Upon information and belief, Defendants failed to employ reasonable safeguards, pursuant to industry standards and commensurate with the highly sensitive nature of the PII at issue, to protect Plaintiffs' and Class Members' PII. As a result of Defendants' failure, Plaintiffs' and Class Members' highly sensitive PII was accessed, viewed, and downloaded by unauthorized third parties in the Data Breach.

70. Defendants flouted scores of guidelines, set forth by government agencies and industry experts and failed to implement them.

71. For example, the FTC has set forth guidelines about reasonable safeguards for data. The FTC's *Start with Security: A Guide for Business* paper instructs companies to "know what personal information you have in your files and on your computers, and keep only what you need for your business, … protect the information that you keep, and properly dispose of what you no longer need," and "create a plan to respond to security incidents."[29]

72. The FTC also instructs business to "take reasonable steps" to keep personal data secure.[30] This includes "put[ting] controls in place to make sure employees have access only on

---

[28] *See* North Shore Univ. Hosp. Northwell Health, *North Shore Univ. Hosp. Sends Notice of Unauthorized Access to Personal Information,* https://nsuh.northwell.edu/sites/northwell.edu/files/2022-02/NSUH-data-breach-media-notice.pdf (Feb. 1, 2022).

[29] Fed. Trade Comm'n, *Start with Sec.: A Guide for Business (2015)*, https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

[30] *Id.*

a 'need to know' basis."[31] The FTC also recommends using "separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases."[32] Moreover, "[i]f employees don't have to use personal information as part of their job, there's no need for them to have access to it."[33]

73. Importantly, the FTC advises companies to "store sensitive personal information securely" especially during transmission.[34] The FTC recommends that companies "use strong cryptography to secure confidential material during storage and transmission." This includes "mak[ing] sure the people you designate to do that job understand how your company uses sensitive data and have the know-how to determine what's appropriate for each situation."[35]

74. Defendants failed to follow the FTC's reasonable guidelines and other industry best practices and, as a result, failed to safeguard Plaintiffs' and Class Members' highly sensitive PII from unauthorized disclosure.

75. Defendants could have prevented this Data Breach by implementing the security and privacy measures recommended by federal and state government agencies and industry organizations. Such measures would have involved proper encryption of Plaintiffs' and Class Members' PII. Moreover, Defendants could have destroyed the data that was no longer needed their services.

76. Upon information and belief, Defendants did not implement reasonable or proper protocols for authorization and access to their networks and systems which contributed to the Data Breach.

---

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*

77. Defendants' failure to safeguard the PII of Plaintiffs and Class Members is made worse by the fact that Defendants were repeatedly made aware of the foreseeable cyber security and privacy risks to the healthcare industry. Despite these clear warnings, Defendants failed to secure and safeguard Plaintiffs' and Class Members' PII.

78. Defendants' failure to protect Plaintiffs' and Class Members' PII from unauthorized disclosure is made even worse by the fact that Defendants admittedly appreciated the grave dangers of identity theft associated with PII. Specifically, Defendant Northwell told the public that, "[a]ccording to a recent industry report, 15.4 million consumers were victims of identity theft or fraud last year, stealing a total of $16 billion dollars from victims. Awareness is key to helping you avoid becoming a victim of identity theft."[36] In making this public disclosure, Defendants assured the public that they were aware of cyber risks. Taken with Defendants' public representations about cyber security and privacy, these public disclosures assured Plaintiffs and Class Members that they could trust Defendants with their PII.

VII. THIS DATA BREACH WILL RESULT IN ADDITIONAL IDENTITY THEFT AND FRAUD

79. Because of the Data Breach – caused by Defendants' misconduct – Plaintiffs and Class Members face an increased (and imminent) risk of identity theft or fraud. In fact, unbeknownst to Plaintiffs and Class Members, they may have already suffered from identity theft or fraud in connection with the Data Breach.

80. Plaintiffs and Class Members face several types of identity theft and fraud including financial identity theft, medical identity theft, criminal identity theft, synthetic identity theft, and child identity theft. These forms of identity theft can result in credit card fraud, fraud

[36] Northwell Health, *supra* at 6.

through government documents and benefits, bank fraud, employment fraud, tax fraud, and medical fraud.[37]

81. The risk of identity theft to data breach victims is pervasive and continues for years after a data breach. According to a 2017 Javelin strategy and research presentation, fraud based on data that is 2 to 6 years old has increased by nearly 400%.[38]

82. Upon information and belief, any relief Defendants purport to provide will not be sufficient in protecting Plaintiffs and Class Members from the imminent risks of identity theft or fraud that they will face for years to come.

VIII. PLAINTIFFS AND CLASS MEMBERS SUFFERED DAMAGES

83. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by HIPPA, various other state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

84. Plaintiffs' and Class Members' PII is private and sensitive in nature and Defendants failed to adequately safeguard the information.

85. Defendants did not obtain Plaintiffs' and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

---

[37] McAfee, *A Guide to Identity Theft Statistics for 2023*, https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/.
[38] Experian, *supra* note 22.

86. As a direct and proximate result of Defendants' wrongful action and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from the possibility of identity theft or identity fraud by hackers and cybercriminals requiring them to undertake additional measures to mitigate the actual and potential impact of the Data Breach on their lives that they would not otherwise have to undertake. Such measures include: (i) implementing credit freezes; (ii) setting alerts with credit reporting agencies; (iii) alerting financial institutions; (iv) alerting medical providers; (v) closing or modifying bank accounts; and (vi) monitoring credit reports for unauthorized activity.

87. Defendants' misconduct directly and proximately caused the Data Breach which subjected Plaintiffs' and Class Members' highly sensitive PII to unauthorized disclosure without their knowledge or consent. As a result of Defendants' misconduct, Plaintiffs and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including: (i) theft of their valuable PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to sufficiently mitigate the risks of identity theft and fraud due to Defendants' untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

88. Because Defendants have not completed their investigation of the Data Breach, Plaintiffs and Class Members face a continued, unknown risk of additional harm which will only be revealed upon Defendants' completion of the investigation.

89. Additionally, Plaintiffs and Class Members face an ongoing risk of harm because Defendants continue to maintain possession, custody, and control over Plaintiffs' and Class Members' PII.

90. While the PII of Plaintiffs and Class Members has been accessed or stolen, a copy of the same PII continues to be held by Defendants. Plaintiffs and Class Members have an undeniable interest in ensuring that this information is secure, remains secure, and is not subject to further breach or theft.

CLASS ALLEGATIONS

91. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

92. The Class the Plaintiffs seek to represent is defined as follows:

> All individuals whose personally identifiable information ("PII") was compromised, accessed, or disclosed in the breach that is the subject of the Notice of Data Breach that Defendants Northwell Health, Inc. and Perry Johnson & Associates, Inc. distributed on or about November 3, 2023 (the "Class").

93. Excluded from the Class are the following individuals and/or entities: (i) any Judge or Magistrate presiding over this action, any members of their immediate families, and any of their staff; (ii) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, assigns, current and former employees, officers, and directors, and any entity in which a Defendant has a controlling interest; and (iii) Plaintiffs' counsel and Defendants' counsel.

94. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the court determines whether certification is appropriate.

95. **Numerosity (Rule 23(a)(1))**: The exact number of members of the Class is unknown and currently unavailable to Plaintiffs, but joinder of individual members herein is impractical. The Class is likely comprised of millions of individuals. According to recent reports, the Data Breach impacted over 3.8 million individuals. Moreover, Defendant PJA has disclosed that the Data Breach impacted over 8 million individuals. The precise number of Class members, and their addresses, are unknown to Plaintiffs at this time, but can be ascertained from Defendants' records. The Class Members may be notified of the pendency of this action by mail or email, internet postings and/or publications, and supplemented (if deemed necessary or appropriate by the Court) by published notice.

96. **Predominant Common Questions (Rule 23(a)(2))**: The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. The common and legal questions include, without limitation:

(a) Whether Defendants had a duty to protect the PII of Plaintiffs and Class Members;

(b) Whether Defendants had a duty not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

(c) Whether Defendants failed to adequately secure and safeguard the PII of Plaintiffs and Class Members;

(d) Whether Defendants timely learned of the Data Breach;

(e) Whether Defendants made an untimely disclosure of the breach to Plaintiffs and Class Members;

(f) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate for the nature and scope of the information compromised in the Data Breach;

(g) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to secure and safeguard the PII of Plaintiffs and Class Members;

(h) Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct;

(i) Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

(j) Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm they face as a result of the Data Breach.

97. **Typicality of Claims (Rule 23(a)(3))**: Plaintiffs' claims are typical of the claims of the Class because Plaintiffs, like all other Class members, had their PII compromised in the Data Breach, suffered damages as a result of that Data Breach, and seek the same relief as the proposed Class Members.

98. **Adequacy of Representation (Rule 23(a)(4))**: Plaintiffs adequately represent the Class because their interests do not conflict with the interests of Class Members, and they have retained counsel competent and experienced in complex class actions and consumer litigation.

99. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class.

100. **Superiority (Rule 23(b)(3))**: A class action is superior to other available means of adjudication for this controversy. It would be impracticable for Class Members to individually litigate their own claims against Defendants because the damages suffered by

Plaintiffs and the members of the Class are relatively small compared to the cost of individually litigating their claims. Individual litigation would create the potential for inconsistent judgments and delay and expenses to the court system. A class action provides an efficient means for adjudication with fewer management difficulties and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class against Defendants)

101. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

102. Defendants required Plaintiffs and Class Members to entrust Defendants with Plaintiffs' and Class Members' PII as a condition of receiving healthcare services.

103. A special relationship exists between Defendants and Plaintiffs and Class Members because Defendants were healthcare providers for Plaintiffs and Class Members, patients of Defendants.

104. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in collecting, obtaining, retaining, storing, securing, safeguarding, sharing, deleting, and protecting Plaintiffs' and Class Members' PII in its possession from being compromised, breached, lost, stolen, accessed, or misused by unauthorized persons or entities. Specifically, Defendants had a duty to: (i) reasonably implement, design, and maintain security and privacy measures or systems to secure and safeguard Plaintiffs' and Class Members' PII; (ii) adequately test Defendants' security and privacy measures or systems; (iii) vet and test the security and privacy measures or systems of vendors to ensure that Plaintiffs' and Class Members' PII was reasonably secured and safeguarded; (iv) implement measures to detect system vulnerabilities, breaches, unauthorized access, or cyber-attacks in a timely manner; (v) implement a reasonable

protocol to respond to system vulnerabilities, breaches, unauthorized access, or cyber-attacks in a timely manner to mitigate risks to Plaintiffs' and Class Members' PII; (vi) timely notify co-Defendants, partners, vendors, and other related entities, regarding vulnerabilities, breaches, unauthorized access, or cyber-attacks to its networks; and (vii) maintain data security measures consistent with industry standards.

105. Defendants' duties arose from the common law and statutes cited herein. Under the law, Defendants had a duty to secure and safeguard Plaintiffs' and Class Members' PII, including confidential health information, and to timely disclose any unauthorized access or theft of PII to Plaintiffs and Class Members. Further, Defendants had a duty to prevent foreseeable harm to Plaintiffs and Class Members. Defendants were aware that the risk of unauthorized access, data breach, or cyber-attack was foreseeable. Defendants were also aware that the PII of Plaintiffs and Class Members was the foreseeable and probable target of unauthorized third parties, such as hackers or cybercriminals.

106. Defendants breached their duty to reasonably safeguard the PII of Plaintiffs and Class Members and their duty to timely notify Plaintiffs and Class Members of the Data Breach. Defendants failed to notify Plaintiffs and Class Members of the Data Breach until November 3, 2023.

107. Additionally, Defendants have failed to provide sufficient information to Plaintiffs and Class Members about the Data Breach despite the fact that it has been months since the Data Breach was discovered. To date, Defendants have failed to: (i) disclose or identify the unauthorized third party or parties; (ii) disclose the network or system vulnerabilities that allowed the unauthorized third party to gain access to Plaintiffs' and Class Members' PII, including confidential health information; (iii) disclose whether Defendants paid a ransom cost to

recover any compromised PII; and (iv) specify the scope of the Data Breach, including the time period during which the compromised data was collected.

108. Defendants breached their duty owed to Plaintiffs and Class Members by, among other things, failing to safeguard Plaintiffs' and Class Members' PII from disclosure to unauthorized third parties. Specifically, Defendants' breach resulted in unauthorized third parties accessing, viewing, downloading, or misusing Plaintiffs' and Class Members' PII.

109. Defendants further breached their duty owed to Plaintiffs and Class Members by failing to provide timely and sufficient notice of the Data Breach to Plaintiffs and Class Members. To date, Defendant Northwell has failed to provide direct notice of the Data Breach to Plaintiffs and Class Members. Defendants did not provide notice of the Data Breach to Plaintiffs and Class Members for months after discovering the Data Breach. Defendants still have not provided adequate notice of the breach because Defendants have failed to: (i) disclose or identify the unauthorized third party or parties; (ii) disclose the network or system vulnerabilities that allowed the unauthorized third party to gain access to Plaintiffs' and Class Members' PII, including confidential health information; (iii) disclose whether Defendants paid a ransom cost to recover any compromised PII; and (iv) specify the scope of the Data Breach, including the time period during which the compromised data was collected.

110. Because of Defendants' untimely notice, Defendants prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII, including, but not limited to medical information and bank account information.

111. Defendants further breached their duty owed to Plaintiffs and Class Members by, upon information and belief, improperly, inadequately, and unreasonably storing the PII of Plaintiffs and Class Members in ways that deviate from governing laws and industry rules,

regulations, and practices. As a result, Defendants failed to safeguard Plaintiffs' and Class Members' PII.

112. Defendants' failure to reasonably and properly safeguard Plaintiffs' and Class Members' PII constituted a breach of their duty to protect PII and prevent unauthorized disclosure or access to PII by third parties.

113. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised, accessed, viewed, downloaded, misused, stolen, or illegally sold by an unauthorized third party or parties.

114. Moreover, Defendants' failure to comply with the applicable laws and regulations constitutes negligence *per se*.

115. Because of Defendants' failure to reasonably safeguard Plaintiffs' and Class Members' PII, Plaintiffs and Class Members suffer injury and damages.

116. Since receiving Defendants' *Notice of Data Breach*, Plaintiffs and Class Members have taken and must continue to take affirmative steps to ensure that their identity and financial information are not stolen or misused. But for Defendants' breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have to take these affirmative steps.

117. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft or fraud due to Defendants' untimely disclosures of

the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

118. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class against Defendants)

119. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

120. Defendants invited Plaintiffs and Class Members to seek healthcare services. Plaintiffs and Class Members accepted Defendants' healthcare services.

121. When Plaintiffs and Class Members sought and accepted healthcare services from Defendants, they were required to provide their PII to Defendants. Plaintiffs provided their PII to Defendants in order to receive healthcare services.

122. As set forth above, Plaintiffs and Class Members entrusted Defendants with their PII, in part, because Defendants repeatedly represented that they would secure and safeguard patients' PII. Upon providing their PII to Defendants, Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to secure and safeguard Plaintiffs' and Class Members' PII and to timely and sufficiently notify Plaintiffs and Class Members of security vulnerabilities, data breaches or unauthorized disclosures.

123. All healthcare services sought by Plaintiffs and Class Members were sought pursuant to mutually agreed-upon implied contracts with Defendants under which Defendants agreed to safeguard and protect Plaintiffs' and Class Members' PII and to provide timely and

sufficient notice if such information was subject to security vulnerabilities, data breaches or unauthorized disclosures.

124. Without Defendants' representations that patient PII would be safeguarded, Plaintiffs and Class Members would not have provided their PII to Defendants.

125. Further, without the existence of the implied contracts, described herein, Plaintiffs and Class Members would not have provided their PII to Defendants.

126. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

127. Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to reasonably secure and safeguard Plaintiffs' and Class Members' PII. Further, Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to timely and sufficiently notify Plaintiffs and Class Members of the Data Breach which resulted in unauthorized disclosures of their PII.

128. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants and Plaintiffs and Class Members, Plaintiffs and Class Members were injured, as set forth herein, and sustained actual losses and damages.

COUNT III
VIOLATIONS OF THE NEW YORK GENERAL BUSINESS LAW § 349, *et seq.*
(On behalf of Plaintiffs and the Class against Defendants)

129. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

130. New York General Business Law Section 349(a) ("Gen. Bus. Law § 349") declares unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state."

131. Plaintiffs and the Class members are "person[s]" within the meaning of N.Y. Gen. Bus. Law § 349(h).

132. Defendants are "person[s], firm[s], corporation[s] or association[s]" within the meaning of N.Y. Gen. Bus. Law § 349(b).

133. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce, in violation of N.Y. Gen. Bus. Law § 349, including: (i) failing to develop, implement, and maintain reasonable security and privacy measures to protect the PII of Plaintiffs and Class Members from unauthorized disclosure; (ii) failing to implement sufficient risk management protocols to mitigate the foreseeable security or privacy risks to Plaintiffs' and Class Members' PII; (iii) failing to reasonably or sufficiently improve their security or privacy measures or systems to reasonably safeguard Plaintiffs' and Class Members' PII from unauthorized disclosure; (iv) failing to comply with legal duties requiring Defendants to reasonably secure and safeguard Plaintiffs' and Class Members' PII, which includes highly sensitive medical information; (v) misleading Plaintiffs and Class Members to believe that Defendants would secure and safeguard Plaintiffs' and Class Members' PII by, among other things, misrepresenting the security or privacy measures or systems Defendants put in place; and (vi) failing to timely or sufficiently disclose the material fact that, because of Defendants' misconduct, Plaintiffs' and Class Members' PII was compromised, subject to the Data Breach, and viewed, accessed, downloaded, misused, or stolen by third parties without their knowledge or consent.

134. Defendants' deceptive acts and practices, including, but not limited to those stated herein, were a direct and proximate cause of the Data Breach.

135. Defendants' concealment of the true timing and scope of the Data Breach was material to Plaintiffs and Class Members.

136. The conduct alleged herein constitutes recurring, "unlawful" deceptive acts and practices in violation of Gen. Bus. Law § 349, and as such, Plaintiffs and Class Members seek monetary damages and the entry of preliminary and permanent injunctive relief against Defendant, requiring Defendants to implement reasonable and sufficient safeguards over patient data to prevent further unauthorized disclosure.

137. Defendants made affirmative misrepresentations to Plaintiffs and Class Members that Defendants were securely collecting, maintaining, and safeguarding patients' highly sensitive PII from unauthorized disclosure. Defendants, however, concealed, and suppressed material facts concerning their unreasonable security and privacy measures, their unauthorized disclosure of Plaintiffs' and Class Members' PII in the Data Breach, and the full scope of the Data Breach.

138. Defendants had an ongoing duty to Plaintiffs and Class Members to refrain from unfair and deceptive practices. Specifically, Defendants owed Plaintiffs and Class members a duty to disclose all the material facts regarding the unauthorized disclosure of their highly sensitive PII, much of which is medical information protected by HIPPA.

139. Plaintiffs and Class Members had no way of discerning that Defendants' representations were false and misleading because Plaintiffs and Class Members did not have access to Defendants' internal technology, data storage, or privacy systems and software.

140. Defendants thus violated Gen. Bus. Law § 349 by making statements that when considered from the perspective of the reasonable consumer conveyed that patients' highly sensitive PII was secure and safeguarded from unauthorized disclosure. Defendants intentionally

and knowingly made affirmative misrepresentations and failed to disclose material facts regarding the Defendants' failure to safeguard patients' PII after discovering the Data Breach months earlier. Defendants knew or should have known that their conduct violated Gen. Bus. Law § 349.

141. Defendants owed Plaintiffs and Class Members a duty to safeguard their highly sensitive PII and alert them of any unauthorized disclosure in a timely manner with specificity.

142. Plaintiffs and Class Members suffered ascertainable loss and actual damages as a direct and proximate result of Defendants' misrepresentations and concealment of and failure to disclose material information. Defendants had an ongoing duty to all customers and the public to refrain from unfair and deceptive practices. Plaintiffs and Class Members incurred or will incur costs including for, among other things, credit freezes, credit monitoring services, or identity theft protection services. Moreover, Plaintiffs and Class Members were injured by Defendants because, among other things, the Defendants' actions caused: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft and fraud due to Defendants' untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

143. Defendants' deceptive and unlawful practices affected the public interest and consumers generally, including millions of New Yorkers affected by the Data Breach.

144. Defendants' deceptive and unlawful practices present a continuing risk to Plaintiffs and Class Members as well as to the general public. Defendants' unlawful acts and practices complained of herein affect the public interest.

145. Plaintiffs and Class Members seek monetary relief against Defendants measured as the greater of (i) actual damages in an amount to be determined at trial, and (ii) statutory damages in the amount of $50 for each Class member. Plaintiffs and Class Members also seek an order enjoining Defendants' deceptive acts and practices, attorneys' fees, and any other just and proper relief under N.Y. Gen. Bus. Law § 349.

COUNT IV
VIOLATIONS OF THE NEW YORK DECEPTIVE SALES PRACTICE ACT
New York Gen. Bus. Law § 350, *et seq.*
(On behalf of Plaintiffs and the Class against Defendants)

146. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

147. N.Y. Gen. Bus. Law § 350 provides, in part, that "[f]alse advertising in the conductof any business, trade or commerce or in the furnishing of any service in this state is hereby declared unlawful."

148. N.Y. Gen. Bus. Law § 350(a)(1) provides, in part, as follows:

> The term "false advertising" means advertising, including labeling, of a commodity, or of the kind, character, terms or conditions of any employment opportunity if such advertising is misleading in a material respect. In determining whether any advertising is misleading, there shall be taken into account (among other things) not only representations made by statement, word, design, device, sound or any combination thereof, but also the extent to which the advertising fails to reveal facts material in the light of such representations with respect to the commodity or employment to which the advertising relates under the conditions prescribed in said advertisement, or under such conditions as are customary or usual.

149. Defendants made statements and omissions that were untrue or misleading. Defendants disseminated such statements through New York. Defendants disseminated such statements and omissions through advertising, marketing, policies, and other publications.

Defendants knew or through the exercise of reasonable care should have known that such statements and omissions were untrue and misleading.

150. Defendants' security and privacy representations contain untrue and materially misleading statements and omissions regarding the adequacy of Defendants' security and privacy measures.

151. Defendants made numerous material and affirmative misrepresentations and omissions of fact with intent to mislead and deceive concerning Defendants' ability to safeguard Plaintiffs' and Class Members' PII. Specifically, Defendants intentionally concealed and suppressed material facts concerning the identification of the Data Breach of Plaintiffs' and Class Members' PII, the scope of the Data Breach, and the reasons for the Data Breach. Defendants knew, based on their own investigations, that the Data Breach occurred and impacted the PII of millions of individuals. Defendants intentionally and grossly defrauded Plaintiffs and Class Members about the security of their PII in Defendants' systems.

152. Defendants made untrue and misleading statements and representations willfully, wantonly, and with reckless disregard for the truth.

153. Defendants' conduct constitutes multiple, separate violations of N.Y. Gen. Bus. Law § 350.

154. Defendants' material misrepresentations were substantially uniform in content, presentation, and impact upon consumers at large. Moreover, all individuals seeking healthcare services were and continue to be exposed to Defendants' material misrepresentations and omissions.

155. Defendants' violations present a continuing risk to Plaintiffs and Class Members. Defendants' deceptive acts and practices affect the public interest.

156. Plaintiffs and Class Members have suffered injury-in-fact and/or actual damages and ascertainable loss as a direct and proximate result of the Defendants' violation.

157. Plaintiffs and Class Members seek monetary relief against Defendants measured as the greater of (i) actual damages in an amount to be determined at trial, and (ii) statutory damages in the amount of $500 for each Class Member, and because Defendants' conduct was committed willingly and knowingly, Class Members are entitled to recover three times actual damages, up to $10,000. Plaintiffs and Class Members also seek an order enjoining Defendants' false advertising, attorneys' fees, and any other just and proper relief under N.Y. Gen. Bus. Law § 350.

COUNT V
VIOLATIONS OF THE NEW YORK DECEPTIVE SALES PRACTICE ACT
New York Gen. Bus. Law § 899-aa
(On behalf of Plaintiffs and the Class against Defendants)

158. Plaintiffs incorporate by reference all allegations in this Complaint and restate them as if fully set forth herein.

159. Defendants are businesses that own, or license computerized data as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a).

160. Defendants are subject to N.Y. Gen. Bus. Law §§ 899-aa (2) and (3) because they maintain computerized data that includes Plaintiffs' and Class Members' PII which Defendants do not own.

161. Plaintiffs' and Class Members' PII includes information protected and covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

162. Defendants engaged in deceptive, unfair, and unlawful trade acts and practices by failing to reasonably safeguard Plaintiffs' and Class Members' PII, prevent the Data Breach, or mitigate the effects of the Data Breach.

163. Pursuant to this statute, Defendants are required to give immediate notice of a breach of a data system to the owners of PII. Defendants do not own the data that was subject to the Data Breach. Thus, Defendants were required to give immediate notice of the Data Breach to Plaintiffs and Class Members.

164. Pursuant to this statute, Defendants are required to sufficiently notify Plaintiffs and Class Members if they discover a security breach or receive notice of a security breach which may compromise PII in the most expedient time possible without unreasonable delay.

165. Defendants failed to timely or sufficiently disclose the Data Breach, a security breach, in violation of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

166. As a direct and proximate result of Defendants' violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiffs and Class Members suffered damages, including: (i) theft of their PII, which includes highly sensitive medical information; (ii) imminent injury from identity theft; (iii) inability to mitigate the risks of identity theft and fraud due to Defendants' untimely disclosures of the Data Breach; (iv) loss of privacy; (v) the payment of costs to remedy or mitigate the effects of the Data Breach, including, but not limited to, payment for credit monitoring services.

167. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for relief and judgment against Defendants as follows:

a. An order declaring this action to be a proper class action, appointing Plaintiffs and their counsel to represent the Class, and requiring Defendants to bear the costs of class notice;

b. An order enjoining Defendants from inadequately safeguarding the PII that remains in their possession, custody, and control;

c. An order requiring Defendants to develop and implement reasonable security and privacy measures, commensurate with the highly sensitive PII they store, in accordance with governing legal and industry standards.

d. An order requiring Defendants to engage in a corrective or remedial advertising campaign to alert patients and consumers about the specific vulnerabilities in their security and privacy systems and the steps being taken to remediate those vulnerabilities;

e. An order awarding declaratory relief, and any further retrospective or prospective injunctive relief permitted by law or equity, including enjoining Defendants from continuing the unlawful practices alleged herein, and injunctive relief to remedy Defendants' past conduct;

f. An order requiring Defendants to pay restitution to restore all funds acquired by means of any act or practice declared by this Court to be an unlawful, unfair, or fraudulent business act or practice, untrue or misleading advertising, or a violation of law, plus pre- and post-judgment interest thereon;

g. An order requiring Defendants to disgorge or return all monies, revenues, and profits obtained by means of any wrongful or unlawful act or practice;

h. Awarding Plaintiffs and the Class compensatory damages, in an amount exceeding $5,000,000, to be determined by proof;

i. Awarding Plaintiffs and the Class appropriate relief, including actual and statutory damages;

j. For punitive damages;

k. Awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

l. Awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

m. Awarding pre-judgment and post-judgment interest; and

n. Granting any other relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: November 21, 2023

Respectfully submitted,

/s/ Michael P. Canty

LABATON SUCHAROW LLP
Michael P. Canty
Carol C. Villegas
Danielle Izzo
140 Broadway
New York, New York 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
mcanty@labaton.com
cvillegas@labaton.com
dizzo@labaton.com

Counsel for Plaintiffs and the Proposed Class